An Evaluation of Controls On Wiretaps and Bugs'

In connection with a survey on "Electronic Surveillance and Wiretapping: Law and Practice 1974," a joint study by the Cornell University Law School and the New York Law Journal, former Justice Arthur H. Schwartz of the New York Supreme Court has prepared a two-part evaluation of federal statutes, court decisions, and other regulations to control abuses in the area of unauthorized interception of private communications.

The first article, published yesterday, described the evolution and interpretation of the law and the use of evidence obtained. In the second article today, Judge Schwartz analyzes procedures for orders authorizing interceptions, statutory damage actions, filing provisions and New York's statutory approach.

Judge Schwartz, a former president of the New York County Lawyers' Association, is presently a member of the Law Revision Commission and the New York State Commission on Legislative and Judicial Salaries and a senior partner in the firm of Schwartz, Burns, Lesser & Jacoby. Alan B. Hyman, an associate in his office, assisted in the preparation of the article.

By Arthur H. Schwartz

Second of two parts.

One important object of the Omnibus Act was to establish procedures and guidelines to be followed by law enforcement agencies in obtaining authorized interceptions of wire and oral communication. These procedures are found in Sections 2516-2519 of the Act.[50]

Applications for Orders Authorizing Interceptions

Under Section 2516, the Attorney General, or any Assistant Attorney General specially designated by the Attorney General, may authorize an application to a federal judge for an order authorizing or approving an interception by the FBI or by a federal agency having responsibility for investigation of the offense as to which the application is made, where such interception will provide evidence of the specific offenses listed in Section 2516.

In addition, the principal prosecuting attorney of any state or political subdivision thereof, if authorized by a statute of that state to make application to a state court judge for an order authorizing or approving interception, may apply to such judge for an order pursuant to Section 2518 of the Omnibus Act and the applicable State Law.

Procedure Outlined

Section 2518 sets forth the detailed procedure with respect to applications for orders authorizing or approving interception of wire or oral communications. In essence, such applications must set forth:

(1) The identity of the investigative law enforcement officer making the application and the officer authorizing the application;

(2) A complete statement of

(Continued on page 4, cols. 1 & 2)

the facts relied upon by the applicant to justify his belief that the order should be issued including details as to the particular offense that has been, or is being, committed;

(3) A particular description of the nature and location of the facilities from which, or the place where, the communication is to be intercepted;

(4) A particular description of the type of communication sought to be intercepted;

(5) The identity of the persons committing the offense and whose communications are to be intercepted (for the most recent interpretation of this provision see *U. S. v. Kahn*, No. 72—1328, U. S. Supreme Court, Feb. 20, 1974);

(6) A complete statement as to whether or not investigative procedures have been tried and failed, or why they appear to be unlikely to succeed or are too dangerous;

(7) A statement of the period of time during which the interception is required;

(8) A full and complete statement of facts concerning all previous applications made to any judge for permission to intercept, and the action taken on all such previous applications.

Action by Judge

Upon such application, if the judge determines that the application satisfies the statutory requirements, an *ex parte* order may be issued authorizing or approving the interception within the territorial jurisdiction of the Court in which the judge is sitting. No order is permitted to approve an interception for any period in excess of thirty days.

Extensions of orders may be granted only upon application in accordance with Section 2518 and the extended period can be no longer than thirty days.

Every order as well as an extension of such order must contain a provision that the authorization to intercept shall be executed as soon as practicable and shall be conducted in such a way as to *minimize* the interception of communications not otherwise subject to interception under the Act. *United States v. Bynum*,[51] contains a full discussion of the area of "minimization"—i e., placing limitation on overhearing "innocent" calls.

Case by Case

The Court in *Bynum* indicated that "minimization" does not insure that *no* protected communication will be intercepted, but, rather, should be viewed as requiring law enforcement officials, subject to court supervision, to exercise their authority in such a manner as will reduce unnecessary monitoring of innocent calls. The Court concluded that questions of "minimization" must be dealt with on a case by case basis.

Section 2518 also provides that any law enforcement officer, as identified in the Act, who determines that an emergency exists with respect to conspiratorial activities threatening the national security or conspiratorial activities of organized crime which requires immediate interception before an authorizing order can be issued, and who feels that there are grounds upon which such an order could be entered, may intercept such communication if an application for an order of approval is made in accordance with Section 2518 within forty-eight hours *after* the interception has occurred. If the application is denied, or in a case where the interception is terminated without an order having been issued, the results of any such interception are treated as having been obtained in violation of the Act.

Procedure For Use in Evidence of Intercepted Communications

Section 2518 prohibits the use in evidence of any intercepted communications in any trial or proceeding in a Federal or State Court, unless each party, not less than ten days before the trial, has been furnished with a copy of the court order and accompanying application under which the interception was approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party against whom the intercepted communication is to be used with the above information at least ten days before the trial, and that the party involved will not be prejudiced by the delay in receiving such information.

Any aggrieved person may move to suppress the contents of any intercepted communication on the grounds that the communication was unlawfully intercepted, or that the order of authorization or approval was insufficient, or that the interception was not made in conformity with the order of authorization. Such a motion must be made before the trial, unless there was no opportunity to make such a motion, or the party making the same was not aware of the grounds of the motion.

Disclosure

Section 2517 of the Act permits an investigative law enforcement officer who, by means authorized by the Act, has obtained knowledge of the contents of a wire or oral communication to use or to disclose such contents to other investigative or law enforcement officers to the extent that such use or disclosure is appropriate to the proper performance of the official duties of such officers.

Any person who has received such information pursuant to the provisions of the Act may disclose the contents of the communications while giving testimony under oath, in any proceeding held under the authority of the United States or of any state or political subdivision thereof.

Section 2517 further provides that when a law enforcement officer, while engaged in interceptions pursuant to the Act, intercepts information relating to offenses other than those specified in the order of authorization, the contents thereof may also be disclosed or used by himself or by another law enforcement or investigative official. An example is found in *United States v. Cox*,[52] where the defendant was convicted of bank robbery on the basis of wiretapping of telephone conversations under an order of investigation relating to possible violation of narcotics laws. The Court held that Section 2517 of the Act rendered the evidence against the defendant admissable.

Section 2517 makes it clear that no otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of the Act loses its privileged character by virtue of interception.

Statutory Damages Actions

Section 2520 of the Act provides a civil cause of action to any person whose wire or oral communication is intercepted, disclosed or used in violation of the Act. The action may be brought against any person who so intercepts, discloses or uses the communication or procures any other person to intercept, disclose or use such communication. The Section provides for the recovery of actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of the violation, or, if higher, $1,000, punitive damages and a reasonable attorney's fee and other litigation costs reasonably incurred.

The American Civil Liberties Union reports several suits for statutory damages currently pending.[53] One such action has been brought by a former National Security Counsel deputy against Henry Kissinger and others. The plaintiff was one of a group of government officials whose telephones were tapped at the order of the White House—allegedly at the request of Mr. Kissinger—as part of a compaign to stop news leaks. Among the actions reported by ACLU are a statutory damage suit brought by several of the defend-

ants in the "Chicago 7" conspiracy case, and suits brought by such organizations as the Black Panther Party, CORE, the Jewish Defense League and National Mobilization Committee to End the War in Vietnam.

In connection with this Section reference should be had to *Kinoy v. Mitchell* [54] which established the standing of persons overheard on warrantless "taps" to bring a civil action for damages under Section 2520 of the Act, even when they are not the subscriber for the particular phone on which the conversation was overheard.

Filing Provisions of the Act

Section 2519 of the Act contains various filing provisions requiring among other things that within thirty days after the expiration of an order entered under Section 2518, or the denial of an order seeking such an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts (the "Administrative Office") the fact that an order, or an extension of an existing order, was applied for, the kind of order or extension applied for, the fact that it was granted, modified or denied, the period of interception authorized, the offenses specified in the order or application, the identity of the applying investigative law enforcement officer and the person authorizing the application and the nature of the facilities from which or the place where communications were to be interpreted.

Data from Prosecutor

In January of each year the Attorney General, or the principal prosecuting attorney of each State, must report to the Administrative Office all of the above required information and a general description of the interceptions made under such orders, the number of arrests and trials resulting from such interceptions, the number of motions to suppress made with respect to the interceptions and the number granted or denied, the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained.

In April of each year the director of the Administrative Office must transmit to Congress a full and complete report reflecting the number of applications made and orders granted.

The 1971 Report on Applications for Orders authorizing or approving the interception of wire or oral communications issued by the Administrative Office reveals that, during 1971, of the 816 applications for intercept orders made to State and Federal judges no original applications were denied.

Breakdown of Applications

Of the 816 applications granted, 285 were signed by Federal judges while 531 were signed by State judges. State judges in New York signed 254 of such orders, or approximately 48 per cent of all orders signed by State judges. Orders signed by State judges in New Jersey numbered 187 or roughly an additional 35 per cent.

The 816 applications filed during 1971 compared with 596 applications filed during 1970 and 301 applications filed during 1969. It is perhaps significant that there was a 37 per cent increase in wiretap applications filed in 1971 over 1970.

The Administrative Office's 1972 Report reveals that during 1972, 860 applications for interception orders were made to State and Federal judges. Four applications were denied and one application was withdrawn. Of the 855 applications granted, 206 were signed by Federal judges and 649 were signed by State judges. State judges in New York signed 294 such orders, representing 45 per cent of all orders signed by State judges, and State judges in New Jersey signed 235 orders, or 36 per cent.

The increase in wiretap applications filed in 1972 over 1971 was only 5 per cent. However, the number of authorizations increased 184 per cent over 1969, the first complete year the Omnibus Act was in effect.

No attempt has been made to estimate how many individual conversations have been overheard, but it is obvious that a single court order can authorize eavesdropping on more than one suspect.

Views of Media

Various recent articles take differing views on the extent of current wiretapping. *New York Magazine* [55] dubbed New York "Wired City" and claimed that in 1972 at least 6,500 New Yorkers "helped make New York number one in electronic surveillance." Other articles (for example the *Wall Street Journal* [56]) state that wiretapping has been on the decline since the passage of the Omnibus Act and point to decreases in use of wiretapping by government agencies and the armed forces to buttress this view.

In any event it is clear that none of the figures quoted include wiretapping activity by private individuals or certain governmental agencies involved in foreign security. Obviously, no figures are available to indicate the extent of unauthorized or illegal interception activity.

In addition to reports to the Administrative Office, the Act provides for the establishment of a National Commission for the Review of Federal and State laws relating to Wiretapping and Electronic Surveillance. Such Commission is to be composed of four members of the Senate, four members of the House and seven non-executive branch appointees selected by the President.

New York Statutory Law

Articles 700 and 710 of the Criminal Procedure Law deal with wiretapping and eavesdropping in New York.[57]

The Commentary to Article 700, which replaces the former Code of Criminal Procedure provisions governing wiretapping, notes that after the adoption of the Omnibus Act, the New York Legislature adopted Article 700 of the Criminal Procedure Law to meet the stringent requirements established by the Omnibus Act with respect to authorized interception.

This Article requires an application to either an Appellate Division justice, a Superme Court justice or a County Court judge in the judicial department, district or county in which the eavesdropping warrant is to be executed for a warrant which may be effective for no longer than thirty days and which may be extended for another thirty days. Such a warrant may be issued only upon a showing of probable cause that a specified crime has been, is being, or is about to be committed. A high degree of particularization is demanded for the application and there are also significant notice and reporting requirements.

Originally, under the old Code Section 813-a, declared unconstitutional by the *Berger* decision, an eavesdropping application could have been made by a District Attorney, the Attorney General or an officer above the rank of sergeant of any police department.

Changes in Amendments

The 1968 Amendments retained the District Attorney and Attorney General as permitted applicants, eliminated police officers but added the New York City Police Commissioner and Superintendent of State Police. The 1969 Amendments deleted the latter two, leaving only District Attorneys and the Attorney General as permissible applicants.

By recent amendment, in addition to the District Attorney or the Attorney General, if authorized by the Attorney General, a Deputy Attorney General in charge of the Organized Crime Task Force may submit an application for such an order.

This change was adopted because

the Organized Crime Task Force was created in 1970 as an agency operating under the aegis of the executive branch of the State government and possesses considerable statewide power in the area of combating organized crime. The

amendment might create some problem under the Omnibus Act which states that applicants for eavesdropping warrants must be "the principal prosecuting attorney of any state or the principal prosecuting attorney of any political subdivision thereof."

Section 700.50 contains notice and reporting requirements; Section 70.30 specifies the form and content of an eavesdropping warrant and Section 700.20 sets forth the requirements for applications for a warrant. All of these Sections closely follow the Omnibus Act.

Motions to Suppress

Article 710 sets forth the procedure with respect to motions to suppress evidence unlawfully obtained. The grounds for such a motion are contained in Section 710.20 which provides that a Court may order that evidence be suppressed if, among other things, it consists of testimony describing conversations overheard or recorded by means of eavesdropping obtained under circumstances precluding admissibility in a criminal action (i. e., not obtained in accordance with Article 700).

Section 700.70 states that, subject to certain exceptions, the contents of any intercepted communications may not be received in evidence or otherwise be disclosed upon a trial of a defendant unless he is furnished, not less than ten days before the commencement of the trial, with a copy of the eavesdropping warrant and accompanying application under which the interception was authorized or approved.

Section 710.40 states that a motion to suppress evidence must, except as set forth in such section, be made with reasonable diligence and prior to the commencement of the trial. Section 710.50 indicates in which courts motions to suppress are to be made and Section 710.60 supplies the procedure with respect to such motions.

As is noted in the Practice Commentary to Section 710.70, dealing with motions to suppress, in order to have standing to make such a motion under the CPL the moving party must not only be an aggrieved party, as defined in the statute, but must also be a defendant in a criminal action.

Inadmissible Evidence

The Civil Practice Law and Rules (CPLR) Section 4506 provides that any evidence obtained by illegal eavesdropping is inadmissible in every civil and criminal forum in New York. Any information derived as a result of illegal eavesdropping is similarly inadmissible.

The Section requires a civil litigant who is aware before trial that evidence obtained as a result of an illegal eavesdrop may be used against him to make a pre-trial motion to suppress such evidence. In order to make such a motion one must be an "aggrieved party" as defined in Section 4506-2. Omitted from the list of aggrieved persons is one whose privacy has not been invaded. Thus, as the Commentary indicates, in an illegally monitored conversation between A and B, if evidence which incriminates C is disclosed, C, as a general rule, would lack standing to attack the evidence. However, if a bug were placed in C's house to obtain evidence against C, he would be an aggrieved person even though the intercepted conversation was solely between A and B.

●

Conclusion

By virtue of the Supreme Court decisions immediately prior to the passage of the Omnibus Act, and by virtue of the Act itself, significant strides have been taken toward eliminating abuses in the area of unauthorized interception of private communications. Although many have attacked the entire rationale upon which the Omnibus Act has been structured,[58] most would agree that the Act clearly delineates the circumstances under which authorized interception is permitted and the manner in which such authorization may be obtained.

Undoubtedly, the most glaring abuses will occur not as a result of the actions of those seeking to make authorized interceptions, but, rather, as a result of actions of those making illegal interceptions. Nonetheless, the provisions in the Omnibus Act making such activity illegal and providing for recovery of damages, criminal sanctions and confiscation of devices manufactured, possessed or sold in violation of the Act should provide substantial aid to law enforcement officers in attacking such activity.

At the very least, both Congress and the Courts have clearly recognized and have taken steps to insure one of our most precious freedoms—the right of privacy.

(Concluded)

---

(50) See United States v. Tortorello, 342 F. Supp. 1029 (S. D. N. Y. 1972), aff'd 480 F. 2d 764 (1973), cert. denied 42 U. S. Law Week 3787 (1973) wherein Judge Milton Pollack discusses the statutory provisions in detail.

(51) 360 F. Supp. 400 (S. D. N. Y. 1973), aff'd 485 F. 2d 490 (2d Cir. 1973).

(52) 449 F. 2d 679 (10th Cir. 1971).

(53) A docket of cases in which the A.C.L.U. has intervened is maintained by the National Staff counsel, to whom we wish to express thanks for making such docket available.

(54) 331 F. Supp. 379 (S. D. N. Y. 1971).

(55) July 9, 1973, Vol. 6, No. 28, at p. 28.

(56) Oct. 8, 1973, p. 1.

(57) No attempt has been made to provide a comprehensive summary of New York case law on wiretapping or the statutes of other states, a subject undoubtedly to be covered by the *Law Journal-Cornell Law School Study*. Similarly, only an outline of the New York Statutory Law has been provided as the backbone of such provisions are markedly similar to the Omnibus Act. See also Penal Law Sections 250 et eq.

(58) See for example, Note 3 Valparaiso U. L. Rev. 89, supra, but see also among other cases U. S. v. Novel 444 F. 2d 114 (9th Cir. 1971); United States v. Cafero, 473 F. 2d 489 (3rd Cir. 1973); and United States v. Whitaker, 474 F. 2d 1246 (3rd Cir. 1973) cert. denied — U. S. —, upholding its constitutionality.